



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/843,901	04/27/2001	Scott R. Shell	50037.20USU1	9891
27488	7590	11/02/2005		
MICROSOFT CORPORATION C/O MERCHANT & GOULD, L.L.C. P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903			EXAMINER HENNING, MATTHEW T	
			ART UNIT 2131	PAPER NUMBER
DATE MAILED: 11/02/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/843,901	Applicant(s) SHELL ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 August 2005.
 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1-28 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 27 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 8/12/2005.

2 **DETAILED ACTION**

3 ***Response to Arguments***

4 Applicant's arguments with respect to claim 1-28 have been considered but are moot in
5 view of the new ground(s) of rejection necessitated by the applicant's amendment to the
6 independent claims.

7 Claims 1-28 have been examined.

8 All Objections and Rejections not specifically set forth below have been withdrawn.

9 ***Claim Rejections - 35 USC § 103***

10 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
11 obviousness rejections set forth in this Office action:

12 *A patent may not be obtained though the invention is not identically disclosed or*
13 *described as set forth in section 102 of this title, if the differences between the subject*
14 *matter sought to be patented and the prior art are such that the subject matter as a*
15 *whole would have been obvious at the time the invention was made to a person having*
16 *ordinary skill in the art to which said subject matter pertains. Patentability shall not be*
17 *negated by the manner in which the invention was made.*

18
19 Claims 1- 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogers et al.
20 (US Patent Number 6,301,484) hereinafter referred to as Rogers, and further in view of Ho (US
21 Patent Number 6148342).

22 Regarding claim 1, Rogers disclosed a computer-implemented method for maintaining
23 configuration information on a mobile device (See Rogers Abstract), comprising: receiving a
24 message including a request associated with configuration information stored on the mobile
25 device (See Rogers Col. 5 Lines 14-36); identifying the source of the received message from data
26 associated with the received message (See Rogers Col. 4 Lines 13-17); determining at least one

Art Unit: 2131

1 configuration setting within the configuration information affected by the received message (See
2 Rogers Col. 6 Lines 45-62); and processing the request associated with the configuration
3 information (See Rogers Col. 5 Line 34-Col. 7 Line 30) but failed to disclose associating a
4 security role with the received message based on the identified source of the received message;
5 inserting an identifier into the received message to identify the associated security role;
6 comparing the associated security role of the received message with a security privilege
7 associated with the at least one configuration setting on the mobile device; and if the associated
8 security role of the received message is in agreement with the security privilege associated with
9 the at least one configuration setting on the mobile device, processing the request associated with
10 the configuration information. However, Rogers did disclose that authentication data may be
11 used to provide security (See Rogers Col. 4 Lines 15-17), but did not disclose any details about
12 the authentication.

13 Ho teaches a messaging system in which access to data is controlled through
14 authentication (See Ho Abstract, Figs. 1-2 and Col. 5 Line 51 – Col. 7 Line 5). Ho teaches that
15 in order to authenticate access via a message, the source of the message is determined (See Ho
16 Col. 6 Lines 16-18), associates a security role with the received message based on the identified
17 source of the received message (See Ho Col. 6 Lines 34-36), inserts an identifier into the
18 received message to identify the associated security role (See Ho Col. 6 Lines 37-49), comparing
19 the associated security role of the received message with a security privilege associated with the
20 requested access (See Ho Col. 6 Lines 54-60), and if the associated security role of the received
21 message is in agreement with the security privilege associated with the requested access,
22 processing the request (See Ho Col. 6 Line 62-65).

1 It would have been obvious to the ordinary person skilled in the art at the time of
2 invention to employ the teachings of Ho in the configuration system of Rogers by utilizing the
3 authentication protocol of Ho to authorize the configuration changes for each feature code. This
4 would have been obvious because the ordinary person skilled in the art would have been
5 motivated to protect against unauthorized changes.

6 Regarding claim 8, the combination of Rogers and Ho disclosed a computer readable medium
7 having computer executable components for managing security on a mobile device (See Rogers
8 Abstract and further it is well known that processors execute computer instructions in order to
9 function), comprising: a stored setting having an assigned security role that identifies a privilege
10 that an entity attempting to access the stored setting must satisfy in order to access the stored
11 setting (See Rogers Fig. 2 Feature Codes, Ho Fig. 1 Element 157 and Col. 6 Lines 54-61); a
12 router configured to receive a configuration message over a wireless communication link, the
13 router being further configured to identify a source of the configuration message and insert a
14 security role identifier into the received configuration message based on the identified source
15 (See the rejection of claim 1 above and Ho Col. 6 Lines 16-18 and 38-49), the router being
16 further configured to pass the configuration message to other components of the mobile device
17 (See Ho Col. 6 Lines 38-49), the configuration message including an instruction that affects a
18 configuration setting (See Rogers Col. 5 Lines 34-36); and a configuration manager configured
19 to receive the configuration message from the router and to parse the configuration message to
20 identify the configuration setting affected by the configuration message (See Rogers Col. 6 Lines
21 46-62 and Ho Col. 6 Lines 54-61), the configuration manager being further configured to
22 compare the assigned security role of the configuration message to security roles assigned to

Art Unit: 2131

1 configuration settings stored on the mobile device (See the rejection of claim 1 above); wherein
2 if the configuration setting identified in the configuration message identifies the stored setting,
3 and wherein if the assigned security role has sufficient privilege to access the stored setting, the
4 configuration manager causes the instruction that affects the configuration setting to be
5 processed (See Ho Col. 6 Lines 54-65 and the rejection of claim 1 above).

6 Regarding claim 13, the combination of Rogers and Ho disclosed a computer-
7 implemented method for maintaining configuration information on a mobile device (See Rogers
8 Abstract; It was also well known that computers have computer executable instructions in order
9 to function), comprising: receiving a configuration message including a header (See Ho Fig. 1
10 Element 112) and an instruction (See Ho Fig. 1 Element 124) associated with a configuration
11 setting stored on the mobile device (See Rogers Col. 5 Lines 14-36); identifying the source of the
12 received message from the header of the received configuration message (See Rogers Col. 4
13 Lines 13-17 and Ho Fig. 1 Element 112); associating a security role with the instruction based on
14 the source of the received message (See Ho Col. 6 Lines 34-36), wherein the associated security
15 role is associated to the instruction by a tag included in the message (See Ho Fig. 1 Element
16 136); comparing the security role of the instruction with a security role associated with the
17 configuration setting stored on the mobile device (See Ho Col. 6 Lines 54-60), and if the security
18 role of the instruction is in agreement with the security role of the configuration setting,
19 processing the instruction (See Ho Col. 6 Line 62-65 and the rejection of claim 1 above).

20 Regarding claim 20, the combination of Rogers and Ho disclosed a computer readable
21 medium within a mobile device, comprising: a data structure associated with a configuration
22 setting being associated with a software component resident on the mobile device, the

1 configuration service provider being responsible for maintaining the configuration setting (See
2 the rejection of claim 1 above and Ho Fig. 1), wherein the data structure comprises: a first field
3 including a security role associated with the configuration setting, the security role of the
4 configuration setting identifying a setting privilege which must be had in order to access the
5 configuration setting (See Ho Fig. 1 Element 132), a second field including a security role
6 identifier, wherein the security role identifier is configured for association with a configuration
7 message (See Ho Fig. 1 Element 136); a third field including a security role associated with the
8 configuration service provider, wherein the security role of the configuration service provider
9 identifies a provider privilege which must be had in order to make use of the configuration
10 service provider, and wherein the third field is configured to determine when the security role
11 identifier matches the security role of the configuration service provider (See Ho Fig. 1 Element
12 157) (See the rejection of claim 1 above).

13 Regarding claims 2 and 14, the combination of Rogers and Ho disclosed that associating
14 the security role with the received message comprises assigning a particular security role based
15 on the source of the message (See the rejection of claim 1 above).

16 Regarding claims 3 and 15, the combination of Rogers and Ho disclosed that the source
17 of the message is identified from authentication and decryption of the received message (See the
18 rejection of claim 1 above and Rogers Col. 4 Lines 13-17 and Ho Col. 6 Lines 16-17).

19 Regarding claims 4 and 16, the combination of Rogers and Ho disclosed that the
20 information within the message includes a shared key that identifies the source of the message
21 (See the rejection of claim 1 above; identifier information).

1 Regarding claims 5 and 17, the combination of Rogers and Ho disclosed that processing
2 the request associated with the configuration information further comprises comparing the
3 security role with another security privilege associated with a configuration service provider, the
4 configuration service provider being responsible for managing the configuration information
5 stored on the mobile device (See the rejection of claim 1 above, Ho Col. 6 Lines 54-60, and
6 Rogers Col. 7 Lines 21-28 wherein each feature code had its own privilege level which needed to
7 be compared).

8 Regarding claims 6 and 18, the combination of Rogers and Ho disclosed that if the
9 security role is not in agreement with the other security privilege the request is not processed
10 (See Ho Col. 6 Lines 54-61).

11 Regarding claims 7 and 19, the combination of Rogers and Ho disclosed that if the
12 security role is in agreement with the security privilege associated with the at least one
13 configuration setting and with the other security privilege associated with the configuration
14 service provider, the configuration service provider processes the request by accessing the
15 configuration information (See Ho Col. 6 Lines 54-63 and Rogers Col. 6 Line 63 – Col. 7 Line
16 6).

17 Regarding claim 9, the combination of Rogers and Ho disclosed a configuration service
18 provider configured to manage at least one configuration setting stored on the mobile device, and
19 wherein the processing of the instruction is performed by the configuration service provider (See
20 Rogers Col. 6 Line 63 – Col. 7 Line 6).

21 Regarding claim 10, the combination of Rogers and Ho disclosed that the configuration
22 service provider has an assigned security role that identifies a privilege that must be associated

1 with an instruction that affects a configuration setting which the configuration service provider
2 maintains (See Ho Col. 6 Lines 16-65).

3 Regarding claim 11, the combination of Rogers and Ho disclosed that the configuration
4 manager is further configured to determine if the instruction that affects the configuration setting
5 is in agreement with the security role assigned to the configuration service provider that
6 maintains the affected configuration setting, and if so, the configuration manager is further
7 configured to pass the instruction to the configuration service provider to be handled (See Rogers
8 Col. 6 Line 63 – Col. 7 Line 6 and Ho Col. 6 Lines 54-65).

9 Regarding claim 12, the combination of Rogers and Ho disclosed that the configuration
10 service provider determines if the instruction is in agreement with the security role assigned to
11 the stored setting prior to processing the instruction, and if not, terminating the processing of the
12 instruction (See Rogers Col. 6 Line 63 – Col. 7 Line 6 and Ho Col. 6 Lines 54-65).

13 Regarding claim 21, the combination of Rogers and Ho disclosed a configuration
14 message received over a wireless communication link between a source of the configuration
15 message and the mobile device, the configuration message including an instruction to access the
16 configuration setting, the instruction having an associated security role based on the source of the
17 configuration message (See the rejection of claim 1 above).

18 Regarding claim 22, the combination of Rogers and Ho disclosed a configuration
19 manager configured to cause the instruction to be processed if the security role of the instruction
20 is in agreement with the security role of the configuration setting (See Ho Col. 6 Lines 54-65).

21 Regarding claim 23, the combination of Rogers and Ho disclosed a configuration
22 manager configured to cause the instruction to be processed if the security role of the instruction

is in agreement with the security role of the configuration service provider (See Ho Col. 6 Lines 54-65).

Regarding claim 24, the combination of Rogers and Ho disclosed a configuration manager configured to invoke the configuration service provider if the security role of the instruction is in agreement with the security role of the configuration service provider (See the rejection of claim 1 above; ie name and password), the configuration service provider being further configured to process the instruction if the security role of the instruction is in agreement with the security role of the configuration setting (See Ho Col. 6 Lines 54-65).

Regarding claim 25, the combination of Rogers and Ho disclosed that the first field further comprises a policy field that identifies the configuration setting as a policy setting (See Ho Fig. 1 Element 132 and Col. 4 Lines 1-9 and further it was inherent that because the settings were in the table, they were identified as policy settings).

Regarding claim 26, the combination of Rogers and Ho disclosed that the policy setting can only be modified by an instruction generated by a particular source (See Ho Col. 6 Lines 16-65).

Regarding claim 27, the combination of Rogers and Ho disclosed that the particular source includes administrative privileges (See Ho Col. 2 Lines 21-33).

Regarding claim 28, the combination of Rogers and Ho disclosed that the policy setting may only be modified locally (See Rogers Col. 6 Line 63 – Col. 7 Line 5).

Conclusion

Claims 1-28 have been rejected.

Art Unit: 2131

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

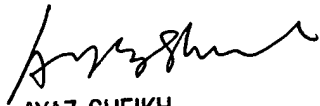
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7
8
9
10
11
12
13 
14
15 Matthew Henning
16 Assistant Examiner
17 Art Unit 2131
18 10/26/2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100